Global Information Assurance Certification Paper

Network Address Translation – Not a Security Panacea
Timothy W. Foreman
November 9, 2000

Abstract

Many end-users and computer professionals consider themselves secure when sitting behind a device that performs Network Address Translation (NAT). This security assumption is flawed in several ways. I intend to demonstrate that NAT, in and of itself, should not be considered a security strategy.

What is Network Address Translation?

Network Address Translation (NAT) is defined in RFC 1631.

NAT was initially created to solve the problem of running out of IP address space due to the explosion of the Internet. NAT is primarily a method of creating private networks of non-routable addresses behind a device that translates these addresses into routable, public addresses to traverse the Internet.

Many people feel that a secondary benefit is that the internal network devices are effectively masked. External programs and "Black Hats" cannot see the internal devices.

Or can they?

Definition of Terms

First, lets define some terms so we are talking about the same things:

NAT Device

> A device that performs Network Address Translation. These devices are varied and can range from a CheckPoint Firewall, a Linux box running IP Chains or a Cisco 675 DSL Router.

Non-Routable Address

> Any IP address selected from the range of addresses defined as non-routable or private in RFC 1597. These addresses are for use on a private network and should never be used on a device that is attached to the Internet. (10.x, 172.16.x – 172.31.x, 192.168.x)

Internal Side

> The side of a NAT device that consists of devices with non-routable (private) IP addresses.

External Side

> The side of the NAT device that is connected to the Internet (or another network.)

Outbound Mode

> When a NAT device is configured to translate internal side addresses to external side addresses, but not to allow external addresses to initiate a connection to any devices on the internal side.

Bi-directional Mode

> When a NAT device is configured to translate specific ports and/or addresses on the external side to internal side ports and addresses thus allowing sessions to be initiated from the external network. Also known as Port Address Translation (PAT).

NAT can be used in several different modes

When NAT is used in Outbound mode, no ports are open for new sessions to be initiated to devices on the internal side of the NAT device. However, this does not completely mask the internal devices. When an internal device initiates a connection to a resource on the external side, the NAT device will allow all packets for this session through to the internal machine. (Provided that the communication continues on the same ports.)

This has several security implications:

1. If a user on the inside initiates a connection to a web site that hosts a malicious application there is nothing on a NAT device that will block or filter the packets that return.
2. There is nothing on the NAT device that will keep "friendly" or malicious applications on an internal host from initiating connections to send data to or request data from an external host. There are many documented "friendly" applications that send information to hosts on the Internet. This could be information that you don't want distributed.
3. NAT does not mask your host information. For example, I run NAT on my home network behind a Cisco 675 DSL router. We are testing Windows Streaming Media at my office. Looking at the log files for the Windows Streaming Media server, I noticed that the entries for my machine contained not only the name of my computer, but also it's internal, non-routable address and the version of the OS I am running. It's very interesting what you can find in the log files of servers for "friendly" applications.
4. It is possible to forge the headers on an IP packet to make it appear that it originated on the internal network side. It is also possible that the NAT device may just forward this packet on into the internal side. This packet could have a malicious payload. (Granted, this is pretty extreme.)
5. Of course NAT provides no virus protection at all.

When NAT is used in Bi-directional mode, or Port Address Translation (PAT) mode, entries are created in a table on the NAT device that map external addresses and ports to internal addresses and ports.

This allows you to setup valid Internet address and port entries on the external side of the NAT device that are statically mapped to private address and port entries on the internal side of the NAT device. Thus you can have a web server on the internal side at address 10.0.0.100 port 80 and have a valid Internet address on the external side of 208.98.45.1 port 80 mapped to it. Any session that is initiated to the external address on port 80 would be forwarded to port 80 on the internal address. Any sessions attempting to connect to other ports that are not explicitly mapped are rejected.

Why is this not a valid method of securing your network?

On the face of it, this seems pretty secure. However, if we look a little harder, we can find some holes.

First off, you still have all the issues associated with Outbound mode as shown above.

However, the biggest hole is that you are allowing connections to be initiated to a server on the internal side from the external side.

But, you say, what good is a web server if people can't get to it? How can I get mail if I don't open port 25?

Many people assume that if they are using NAT, they can forget about firewalls and DMZs and service networks. What they tend to forget is that anytime you allow a session to be initiated from an external network you open yourself up to attack. Many attacks come through the "well known" ports. Most networks are going to have a few well known ports open, such as 80 for HTTP, 25 for sendmail, 20 and 21 for FTP, 53 for DNS, possibly 110 for POP, 143 for IMAP and maybe 23 for telnet. Many exploits are based on the fact that some versions of the programs that run on these ports are insecure and have weaknesses that can be exploited. NAT does nothing to address this.

In addition, many NAT devices don't log the connections from external addresses to internal addresses. If you are depending on a Cisco 675 DSL router performing NAT to keep your network safe, you might be getting attacked and not even know it.

Consider this scenario

I have a router that does NAT. I let in port 80 in to my Web server, port 52 in for DNS, port 23 in for telnet, and port 25 in to my mail server. I think that because I have NAT, and I have all other ports closed to the outside world I am pretty safe. Because I feel safe, I don't setup my web, DNS, telnet and mail servers in a DMZ or a service network, I just hang them off the same wire as the rest of my machines. I feel pretty secure, after all no one can see the machines because they are hiding behind a NAT device, so I don't pay as much attention as I should to keeping the

servers patched up to date.

Along comes a "Black Hat" who sniffs my network. He discovers that I have ports 80, 52, 23 and 25 open and decides to look a little harder. He discovers that I am running RedHat 6.0 with BIND 8.2 for my DNS server and he knows an exploit for it. This is easy enough to find out, there are plenty of tools that will connect to port 53 and ask it.

So, he fires up his tool kit and gets to work.

First he exploits my DNS server via buffer overflow attack. This gives him root access to the box and he installs a couple of new accounts so he can login again later via the telnet port which I so thoughtfully left open for him.

Then he ftps to another server and downloads and installs a back door program that will give him access to the box even if I discover and remove the new accounts.

Finally, he ftps to yet another server and downloads and installs the Trinoo client and starts it up.

After he is all done with this, he cleans up his tracks pretty well by cleaning out the log files.

I have no idea that these events have occurred since I have no intrusion detection system, no logging on the NAT device, and the hacker has covered his tracks pretty well. I may not even discover it for a day or two and by then the hacker could have leap-frogged his way around my internal network or used my network as a base for attacks on other networks. All through ports 53 and 23.

Consider these other scenarios

One of your users happens to run across a web page containing cute little animated programs that she can run on her machine, like "Elf Bowl". Unknown to this user, when she runs the program it installs a trojan on her machine that initiates connections to a server on the external side to get instructions or download more code. Since these sessions are initiated from the inside, the NAT box allows the code in and I won't find out about it until it's too late.

And then there is always that one Executive who has to have a modem so he can dial into AOL to check his mail. Modems present a perfect situation for a hacker to make an end-run around your NAT device (or firewall for that matter.)

Conclusions

NAT, in and of itself, is not a security strategy. Sure it helps by hiding all of your hosts. It closes all the ports that you are not manually opening. But, as I hope I have pointed out, there are still outstanding security issues when using NAT.

Even when you are using NAT, you should have a firewall, a DMZ and an Intrusion Detection System. Otherwise you are flying blind and the first sign that you have been hacked may be when your ISP comes calling asking why your systems are assisting in a DoS attack.

Sources

Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.
URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc1631.html (02 Nov 2000)

Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999. URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc2663.html (02 Nov 2000)

Gibson, Steve. "The Anatomy of File Download Spyware" 10 Oct 2000
URL: http://grc.com/downloaders.htm (02 Nov 2000)

Spitzner, Lance. "The Study of an Attack - Know Your Enemy: A Forensic Analysis", 23 May 2000 URL:
http://www.enteract.com/~lspitz/papers.html (06 Nov 2000)